

EXHIBIT B

since 2005. My primary responsibilities as a TFO are to investigate Human Trafficking crimes. During my tenure as a Columbus Police Officer/Detective/Task Force Agent, I have worked multiple investigations regarding Narcotics, Prostitution and Human Trafficking offenses.

4. I also have specialized training in the area of Human Trafficking, Pimp Controlled Prostitution, Organized Prostitution, Child Prostitution Rings, Narcotics Trafficking and Money Laundering. I have participated in the execution of search warrants and arrests related to the above-referenced offenses. By virtue of my experience and training, your affiant is familiar with money laundering techniques utilized by individuals involved in illegal activities, such a narcotics and human trafficking. Throughout this affidavit, reference to "investigators" specifically refers to criminal investigators.

5. I have participated in several drug trafficking, money laundering, and organized crime investigations that have resulted in the arrest of numerous members of several different domestic drug trafficking organizations as well as the seizure of currency, assets, and controlled substance related to these investigations. Some of these investigations used judicially authorized electronic surveillance as an investigative technique and I have participated in investigations in support of those judicially authorized electronic surveillance operations. Additionally, I have testified on numerous occasions in grand jury proceedings, procedural hearings, and in criminal trials related to the prosecution of individuals involved in sex trafficking offenses.

6. Through instruction, training, and participation in investigations, I have become familiar with the manner and methods by which narcotics traffickers and sex traffickers conduct their illegal business and the language and terms that are used to disguise conversations about their illegal activities. Moreover, narcotics traffickers and sex traffickers frequently use telephone communications to further their illegal activities by, among other things, remaining in constant communication with one another, either verbally or via text messaging.

7. I am also aware that drug traffickers and sex trafficking organizations utilize texting applications to generate multiple phone numbers, at no cost, to communicate. The texting applications can aide to protect trafficker's identities as well. I am also aware that drug traffickers and sex traffickers often utilize more than one communication device at one time in order to facilitate their drug illegal activities.

PURPOSE OF THE AFFIDAVIT

8. The facts and statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Columbus Division of Police Detective and HSI TFO. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have not omitted any facts that would negate probable cause. I have set forth only the facts that I believe are necessary to establish probable cause for a search warrant for the content of one digital media device, specifically a teal Cricket cellular phone with associated IMSI:3101507595093607 belonging to [REDACTED] that was seized from the residence of 334 South Burgess Avenue Columbus, Ohio 43204 after the execution of a residential search warrant on October 13, 2023 (herein after referred to as the **SUBJECT DEVICE**). The device is being held in a secure location at the United States Postal Inspection Services Evidence Storage Facility

9. The **SUBJECT DEVICE** and additional documents to be searched are more particularly described in **Attachment A**, for the items specified in **Attachment B**, which items constitute instrumentalities, fruits, and evidence of violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking). I am requesting authority to forensically examine the entirety of the **SUBJECT DEVICE**, wherein the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

APPLICABLE STATUTES AND DEFINITIONS

10. Title 18, United States Code § 1591 makes it a federal crime for any person, in or affecting interstate or foreign commerce to recruit, entice, harbor, transport, provide, obtain, advertise, maintain, patronize or solicit, by any means, a person, knowing, or in reckless disregard of the fact that the person has not attained the age of 18 years and will be caused to engage in a

commercial sex act. Section 1594 of the same title prohibits attempts or conspiracies to engage in such acts.

11. Pursuant to Title 18, United States Code, Section 1591(e) (3) the term “commercial sex act” is defined as “any sex act, on account of which anything of value is given to or received by any person.”

12. The term “computer”¹ is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

13. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

14. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

15. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

16. As it is used throughout this affidavit and all attachments hereto, the term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

¹The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

**BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES,
MOBILE APPLICATIONS, AND THE INTERNET**

17. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

18. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

19. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

20. Digital devices are also capable of sending and receiving messages. Messages can be received or sent on digital devices in a variety of manner, including, but not limited to, e-mail, texting (including "SMS" and "MMS" messaging), and application messaging (including, but not limited to, Facebook Messenger, Snapchat, and WhatsApp).

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile

device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.

22. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

23. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

24. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes.

Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

25. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment B**.

26. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include Facebook Messenger, Snapchat, and Instagram.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- A. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the

stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

- B. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

INVESTIGATION AND PROBABLE CAUSE

29. On or about April 8, 2023, a Columbus Division of Police (CPD) officer encountered a cooperative source (herein identified as CS#1) who advised that an individual that goes by the street name [REDACTED] is trafficking drugs and women. CS#1 indicated that [REDACTED] was primarily operating his criminal activity on the west-side of Columbus, Ohio. CPD was familiar with the individual CS#1 identified as [REDACTED] from prior law enforcement interactions. More specifically, [REDACTED] was known to law enforcement as [REDACTED] and his drug activities on the west-side of Columbus had been documented by CPD. For example, on or about April 6, 2023, CPD officers executed a search warrant at 390 Clarendon Avenue in Columbus, Ohio, a residence previously associated with [REDACTED] and recovered at that search warrant were approximately three firearms and numerous suspected narcotics to include

crack cocaine, powder cocaine and fentanyl were seized. CS#1 further informed CPD that he/she has been purchasing crack cocaine from [REDACTED] for approximately two to three years. CS#1 stated that during that time frame, he/she knows [REDACTED] to facilitate the posting of online sex advertisements of several women, and that the women then engage in commercial sex acts for profit as a result of these advertisements. CS#1 specifically named two adult females that were currently being promoted for prostitution at the direction of [REDACTED]. CS#1 stated that [REDACTED] will control the money that is earned from these prostitution services and will provide the women with illegal drugs in order for them to continue to engage in the prostitution activities.

30. In or about June 2023, United States Postal Inspectors and Central Ohio High Intensity Drug Trafficking Area (HIDTA) Task Force Officers in Columbus, Ohio initiated a drug trafficking investigation after identifying a pattern of suspicious USPS Priority Mail Express parcels originating in Metro Phoenix Arizona and destined for addresses in Columbus, Ohio. Throughout this investigation, federal agents identified [REDACTED] as the recipient of those packages which included kilogram amounts of fentanyl that was being distributed from a source of supply in Phoenix, Arizona. In addition, legal process that had been served during the course of the investigation revealed that [REDACTED] had also actively tracking the parcels of drugs being shipped to him and picking up those packages upon their arrival to various west-side location in Columbus. Additionally, federal agents believed [REDACTED] was receiving the bulk illegal narcotics through the mail and then redistributing the fentanyl to street level users in the Columbus, Ohio area. For example, throughout the course of that investigation, United States Postal Inspectors tracked packages containing fentanyl to the residence of 334 South Burgess Avenue Columbus, Ohio. The address of 334 S. Burgess Avenue was attributed to [REDACTED] through surveillance methods which observed [REDACTED] receiving the packages. On or about September 28, 2023, law enforcement observed [REDACTED] place numerous bags of trash in a container outside the address. A trash pull that same day resulted in the recovery of, among other things, used latex gloves and one baggie of a white powder/white rock-like substance further corroborating the fact that [REDACTED] was likely redistributing the fentanyl.

31. On October 13, 2023, the Central Ohio High Intensity Drug Trafficking Area (HIDTA) Task Force executed a federal search warrant at 334 South Burgess Avenue in

Columbus, Ohio. This address was known by law enforcement to be a location used by [REDACTED] to receive parcels of drugs in the mail. Entry into the residence was made by the Columbus Ohio Division of Police "INTAC" unit. Upon execution of the search warrant, five individuals, including [REDACTED], were encountered in the residence and detained.

32. During the search of the residence, items indicative of the manufacturing and distribution of controlled substances were found, including, but not limited to: approximately 500 grams of a pressed white powder inside a vacuum sealed bag, digital scales, a loaded AR-15-style rifle, baggies full of white powder, a loaded Glock handgun, approximately \$2,417.00 in a duffle bag, numerous cell phones, numerous Naloxone packages, and fentanyl test strips. Additionally, during the search of the residence, investigators discovered two makeshift rooms in the basement. These rooms were secured shut by a padlock and hasp from the outside of the room. Inside of these rooms were personal items utilized primarily by females. Through training and experience, your affiant is familiar that sex traffickers will use locks in this manner with the intention of keeping someone contained within an area against their will.

33. The federal search warrant obtained for the residence of 334 S. Burgess Avenue also encompassed the search, seizure, and forensic review of any cellular devices recovered from inside the residence. A total of five digital media devices were seized accordingly. Once the devices were seized, the CPD Digital Forensics Unit (DFU) preformed a forensic extraction on the cellular devices to export the data to a Cellebrite Report from each individual phone.

34. Your affiant began the review of the Cellebrite report attributed to a teal Cricket cellular phone with an associated IMSI number of 3101507595093607, belonging to [REDACTED] (the **SUBJECT DEVICE**). [REDACTED] was one of the individuals who was located in the basement of 334 South Burgess at the time the search warrant was executed. Contained within the **SUBJECT DEVICE** Cellebrite report, specifically in the "User Account Information", your affiant identified several social media applications, banking applications and email accounts associated with Amber Braham.

35. While reviewing the Cellebrite report for the **SUBJECT DEVICE** for evidence related to the drug trafficking crimes encompassed in the original federal search warrant, your affiant noted potential evidence of crimes related to sex trafficking or conspiracy to commit sex trafficking. More specifically, your affiant observed messages between [REDACTED] and other

unknown individuals who appeared to be purchasing sex. In these messages observed by your affiant, Braham was arranging meetings with individuals to engage in sex with them through what appeared to be online internet escort advertisements. Your affiant also observed images stored within the device which depict partially clothed to fully naked women posing in sexually provocative positions. Your affiant is familiar with images like these and through training and experience, know that such images are often posted on the internet as advertisements to engage in commercial sex acts. These images depicted Braham and other women not known to your affiant at this time.

36. Based upon the conduct of individuals involved in prostitution such as [REDACTED] in conjunction with the information provided by CS#1 and the drug trafficking activities of [REDACTED] outline above as well as your affiant's training and experience, your affiant has reason to believe that females, such as [REDACTED] may have been engaging in sex acts with individuals in exchange for money from which [REDACTED] profited and that she and others may have been engaging in such activities by means of force, fraud and coercion due to the drugs recovered at the Burgess residence as well as the locks on the outside of the doors of the rooms in the basement of the residence. Your affiant therefore submits that there is probable cause to believe the evidence of violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking) will be located on the **SUBJECT DEVICE**.

SEARCH METHODOLOGY TO BE EMPLOYED FOR DIGITAL MEDIA DEVICES

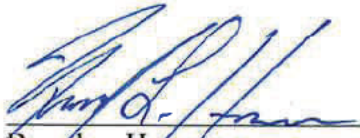
37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

- A. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
- B. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
- C. Surveying various files, directories and the individual files they contain;
- D. Opening files in order to determine their contents;
- E. Scanning storage areas;
- F. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- G. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

38. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

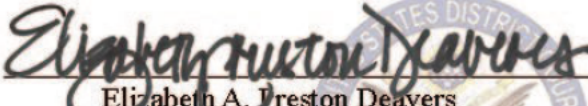
AUTHORIZATION REQUEST

39. Based on all the forgoing information, there is probable cause to believe that violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking) have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICE** listed in **Attachment A**. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICE** described in **Attachment A**, and the seizure of the items described in **Attachment B**.

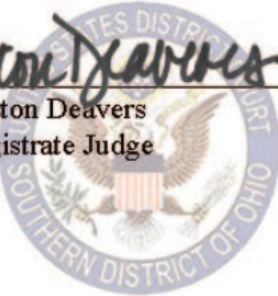


Brandon Harmon
Task Force Agent
Homeland Security Investigations

Sworn and subscribed before me this 9th day of November, 2023.



Elizabeth A. Preston Deavers
United States Magistrate Judge



ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED

The devices to be searched are listed as follows:

One teal Cricket cellular phone with associated IMSI:3101507595093607 belonging to [REDACTED] [REDACTED] that was seized from the residence of 334 South Burgess Avenue Columbus, Ohio 43204 after the execution of a residential search warrant on October 13, 2023. The device is being held in a secure location at the United States Postal Inspection Services Evidence Storage Facility

This warrant authorizes the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
INFORMATION TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking), including but not limited to all electronically stored or recorded/handwritten data on the **SUBJECT DEVICE** or other items as described in

Attachment A and also:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. List of customers and related identifying information;
3. Types, amounts, and prices of drugs as well as dates, places, and amounts of specific transactions;
4. Any information related to source of drugs (including names, addresses, phone numbers, or any other identifying information);
5. Any information related to travel or schedule, particularly for the purpose of obtaining quantities of narcotic drugs or scheduling sex in exchange for money;
6. All bank records, checks, credit card bills, account information, and other financial records;
7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs, and electronic messages,) pertaining to the charges listed above.
9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an

Internet Service Provider or Electronic Communications Service, including any social media accounts.

10. Any and all messages, emails, voicemails, texting applications, text messaging, or social media communications pertaining to prostitution or sex trafficking, including, but not limited to, hotel/motel reservations, car services, posting of prostitution advertisements, and communications regarding the scheduling of dates or payment for sexual services.
11. Any and all lists of names, telephone numbers, and addresses related to the operation of sex trafficking/prostitution services and drug trafficking.
12. Any and all records, files, or documents showing dominion, ownership, custody, or control over the **SUBJECT DEVICE** or other items seized as outlined in **Attachment A** including evidence showing user attrition at the time the things described in the warrant were created, edited, deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history and in addition, the following:
 - a. logs, phonebooks, saved usernames and passwords, documents, and browsing history, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the **SUBJECT DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the **SUBJECT DEVICE** was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the **SUBJECT DEVICE** of other storage devices or similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICE**;
 - h. evidence of the times the **SUBJECT DEVICE** was used; and
 - i. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICE**.
13. Any other forms of storage media and other system components to include mobile applications, global positioning system history, memo and notes, and all indicia, documents and records of co-conspirators, and any other individuals or business with whom a financial relationship exists and the authority to put any electronically stored data and/or items in human viewable form.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement, including the FBI, may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.